Improve Performance Using Dynamic Scheduling Algorithm with Enhancement Security

Shivani Dixit
Student of M.tech (CSE)
Rayat-Bahra University
Mohali,India

Gurbhej Singh
Assistant Professor (CSE)
Rayat-Bahra University
Mohali,India

Abstract: Nowadays in the cyber world & in the world of network communication, security & reliability both are non-replaceable aspects. Modern real-time wireless networks require high-security level. Moreover, with an adaptation of wireless communication technologies in industries/organizations, granting reliability & security for transmission over wireless error-prone medium has become a great challenge. High level of security ensures the confidentiality of information and data stored in packets which are delivered through the wireless network. However, most existing priority based algorithms in real time wireless networks ignore the various security requirements of the packets. Therefore, to overcome those conditions & to provide a better solution to the said problem we are proposing a dynamic scheduling algorithms which ensure a great reliability with high security Applied solution is capable of achieving high quality of security for real-time packets while making the best efforts to guarantee the real-time requirements of those packets i.e. deal lines. We have conducted extensive experiments with the help of simulator to evaluate the performance of our algorithm. Results show that the proposed algorithm can improve both quality and level of security and real-time packet delivery successful ratio.

Keywords: *Scheduling algorithm (EDF), packets drop and loss, Network Security.*

I. INTRODUCTION[1]

Wireless is not intended to replace wired data communication but instead to be utilized in areas that it would be otherwise impossible to communicate using wires. Only recently has the industry been taking steps to formulate a standard that is more suitable for data transmission. Some of the advantages of wireless networks are stated below, which clearly indicates the strong nature of wireless against wired networks across the globe [6].

- Data Integrity - relatively error-free transmission.
- Speed - as close as possible to the speed of current wired networks.
- Protection - making sure that the data now airborne is encoded and cannot be tapped by unwelcome receivers.

Wireless networks are more flexible, adaptive & having more dynamicity in compare to wired ones. However, with all adaptiveness & advantages, there are some major concerns against wireless networks which are.

- Data/information security.

- Dynamic packet categorization & treatment to get perfect, fast & error free delivery.

Data/information security is a major concern in any form of communication. Wireless networks involve the risk of modification and eavesdropping. So, they make use of certain encryption techniques for security. Dynamic real-time packet scheduling technique which reduces packets drop, increase guarantee ratio of data traffic and provide security for data packets. The two main approaches are used in this paper,

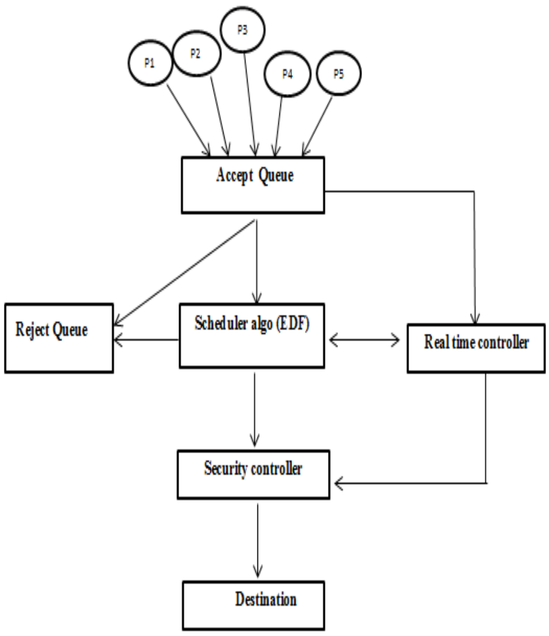
- Scheduling algorithm
- Security

The first contribution of this paper is providing dynamic priority scheduling is a type of scheduling algorithm in which the priorities are calculated during the execution of the system. The goal of dynamic priority scheduling is to adapt to dynamically changing progress and form an optimal configuration in a self-sustained manner. It can be very hard to produce well-defined policies to achieve the goal depending on the difficulty of a given problem. In real time systems, correct computational results generated on time are required for a system to work properly. With wide applications of real-time systems need for high computing hardware platform is also there [3], [4].

The second contribution of this paper is providing security to the data in real time system network. security has become an increasing problem in the world of computer networks, Security becomes essential in wireless computing. especially since the data is broadcast to the receiving unit. International Standards Organization (ISO) has published security services which provide for secure data and computer systems on standard wire line networks. However, these must be modified to meet the needs of mobile users and systems. Data encryption and two possible solutions include exchanging security information between a small number of entities, and even more complex involving an information center.

The remainder of this paper is organized as follows. Section 2 design model. Section 3 discussed the previous paper. Section 4 simulation works. Section 5 future scope and conclusion.

II. DESIGN MODEL



Design model of scheduling algorithm with security

A. Packets Model

A packet contains a segment of data, which is carried in the packet body, or payload. The network programs that assemble the packet follow network protocols that dictate information that should accompany the data in the packet. This data goes into a structure on the front of the packet, called a header. Each data packet has several headers. The packet headers are counted as part of the packet size. The size of the header varies according to which applications use the data and which protocols are used to transport it. The larger the packet header, the smaller the maximum size of the data segment carried by the packet. Packet headers represent an overhead, and so one school of thought recommends that packets be made as large as possible to reduce the percentage of overhead per packet [4][7]. Packet loss or drop occurs when one or more packets are lost during the data transmission across the computer network. Packet loss or drop is either caused by an error in data transmission, network congestion or packet timeout. In TCP connection will need to resent the loss packets but in UDP is not possible.

In the priority queue, the tasks are always kept sorted according to the proximity of their deadline. When a task arrives, recorded a total number of tasks in the priority queues. At every scheduling point, task accepts than move forward otherwise task is rejected.

B. Scheduler Model

The earliest deadline can guarantee higher network utilization than fixed-priority schemes like Deadline, but it is difficult to implement in local area networks. The reason is the need for updating the deadlines (priorities) at each scheduling round and the limited number of priority levels offered by the scheduler. This deadline encoding problem results in an additional priority inversion factor when considering the schedulability analysis of hard real-time messages. This paper describes an effective deadline method and discusses its effects on the guaranteed ratio or system performance.

Scheduler queue would contain the absolute deadline for the task. At every preemption point, the entire queue would be scanned from the beginning to determine the task having the shortest deadline [7].

When EDF is used to schedule a set of periodic real-time tasks, a task overshooting its completion time can cause some other task(s) to miss their deadlines. It is usually very difficult to predict during program design which task might miss its deadline when a transient overload occurs in the system due to a low priority task overshooting its deadline. The only prediction that can be made is that the task (tasks) that would run immediately after the task causing the transient overload would get delayed and might miss its (their) respective deadline(s). However, at different times a task might be followed by different tasks in execution. However, this lead does not help us to find which task might miss its deadline. Even the most critical task might miss its deadline due to a very low priority task overshooting its planned completion time.

C. Security Controller

The real-time controller notifies security level controller to work. The security level controller strives to increase the security level of packets in the accepted queue, which efficiently utilizes the system resource to enhance the security of packets in wireless networks [6]. Security controller adds the security on the data packets and in this paper, we use four key to secure data i.e. random key, symmetric key, public key, crypt hashing function. Packet searches the key according to the priority.

D. Real-time Controller

The real-time controller in the schedule gets a new packet from the schedule queue based on the earliest deadline first (EDF) policy and determines whether or not a new packet can be accepted. To be noted that the real-time controller considers both the new packet and packets waiting in the accepted queue to maximize the schedulability. If the new packet cannot be accommodated, it will be dropped into the rejected queue. Otherwise, it will be transferred to the accepted queue.

III. RELATED WORK

In [1], the author purpose assigned the available bandwidth to the different task means assigned a maximum number of retransmission and suitable portion of the network bandwidth is reserved .according to this approach message delivery source to destination is successful and the pre-allocated bandwidth can be reused to improve the system performance and EDF scheduler help to reuse the pre-allocated bandwidth.

Unfortunately, this kind of approach suffers from main three drawbacks. Firstly, when we are blocking some of the bandwidth from the complete pipe or let’s say complete capacity then somewhere we are degrading the link or transmission medium capability to carry traffic/data/information. Just to secure retransmission if we block some of the bandwidth then we are lacking somewhere for sure. Instead of impacting complete transmission medium now a day's communication is catering to the type of application/protocol & nature of data. For example, if there is a stream of video packets then the sender always sent the data in RTP or UDP mode. Packets are traveling through UDP standard and there is no need for retransmission. If there will be retransmission then many gigs or Tera bites link will not be enough to send the complete trail of packets. So, according to nature of communication & application the desired information/data will be sent in accordance with their nature of formats i.e.TCP, UDP, RTP, unicast, multicast, broadcast and etc.

The second approach is QOS in base paper only implies the overall performance. However, in real-world QOS is quality of service which is implemented as COS (class of service) in MPLS (Multi-protocol label switching) networks & another mode is to implement in a priority based structure i.e. in packet/switched networks (ISP). Here in advance paper, we have packet/switched network and in the sake of that EDF is implemented to enhance the packet delivery with the help of priority based QoS mechanism.

The third approach is Transmission of information/data is carried out in sense of packets in a packet/switched/data network, to provide more reliability & to increase the delivery ratio now we are using a dynamic algorithm to achieve the desired output/goal. Only securing the bandwidth for retransmission from the complete link/capacity will not give the immense/desired output. Hence prioritizing the packet according to need or packet life will give more perfect results.

IV. SIMULATION WORK

The system consists of some main components, throughput, Delay, PDR, jitter sum, lost or drop packets .all are dependent upon the total packet and received a packet on the network and tell the system performance. There are many factors affect the system performance requirement in the processing time of the schedule , so by the fixing time deadline and the time intervals between the data packets, the system was executed for different values of the processing time, in this scenario we have fixed deadline to be 10s,25s,100s,250s.

Time	10 s	25s	100s	250s
Tx	1778	4778	19778	39978
Rx	1662	4662	19662	39862
Delay	.003036	.002962	.003004	.0028442
Jitter	1.41185	1.83188	5.46422	8.30869
Lost /drop	116/0	116/0	116/0	116/0
PDR.	93%	97%	99%	99%
Thx. (kbps)	7002	43002	178002	359802

Tx = Total Packet.

Rx = Received Packet.

PDR = Packet Delivery Ratio

Thx = Throughput

Bj = Base work

Pj = IPSAES (Improve performance using scheduling algorithm with enhancement security).

The first data to be analyzed is the throughput on the fixed processing time. The data packets are moved successfully from source to destination in processing time and typically measured in bits per second (bps), as shown from fig. 1, the throughput increases when increasing time.

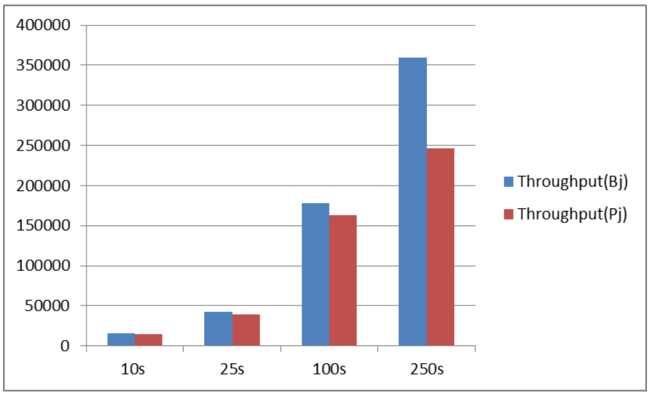


Fig. 1 Comparison of throughput

The second data to be analyzed is total packets delays in given time, as shown from fig.2 the changes of the total delay remain relatively small as compared to the Bj in processing time. Relative changes of Pj clearly indicating the degradation of delay.

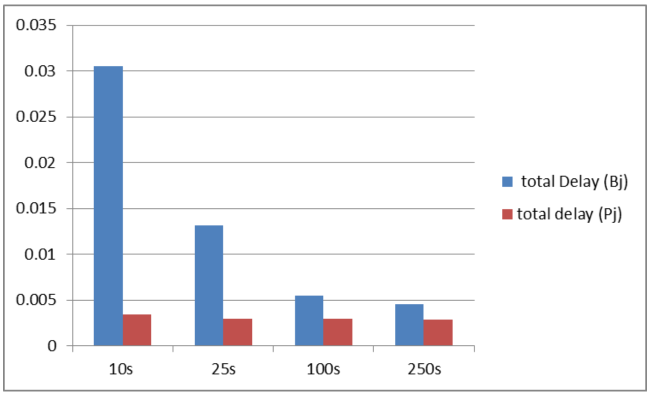


Fig. 2 Comparison of total delay

The third data to be analyzed Jitter is measuring time difference in packet inter-arrival time. It is simply the difference in packet delay. It only impacts the bigger packet switched network. As a time, shift phenomenon, it usually does not cause any communication problems. Actually, TCP/IP is responsible for dealing with the jitter impact on communication. VOIP environment sometimes can be impacted due to this only.

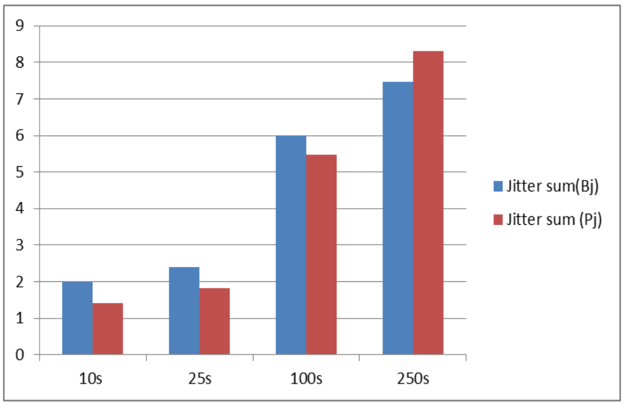


Fig. 3 Comparison of Jitter sum

Comparison study

Performance is directly proportional to the packet delivery will attain higher performance of the network and its mechanism. Here, from Fig 2, we can see that the packet delivery percentage of Bj is 79% and Pj is 93% .both the calculation is recorded at a time interval of 10s .so the performance will be :

Performance = 93% / 79% =1.177

This means that the Pj is better than the Bj by a factor of 1.177.

PDR = TOTAL PACKET TRANSMIT

--- * 100

TOTAL PACKET RECEIVED

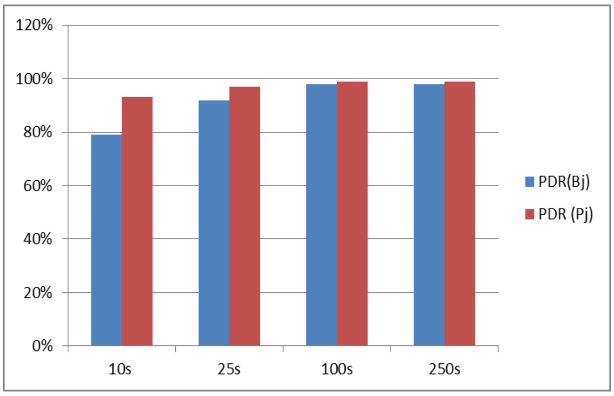


Fig. 4 Comparison of performance

The Second requirement and objective are to reduce the delay in packet delivery. As shown in Fig. 4 ,Delay in packet deliver clearly indicates towards the slowness of network. The slowness of network or in packet delivery tends to multiple issues in reference to real-time applications and services. Today's world real-time applications and services required a high rate of error-free packet delivery for example- voice, video, content sharing. Hence as per the figure 2, there is a recorded delay of 0.030498 seconds for Bj (Base work) and 0.00342 recorded for Pj (Proposed work) in a 10 seconds time interval. In Proposed work, EDF is implemented which signifies the better packet delivery mechanism with lesser delay and less probability of errors.

Delay = .030498/.00342 =8.918

This means that the Pj is better than Bj by a factor of 8.918(times better).

V. CONCLUSION

In this paper a simple real time scheduling algorithm (EDF) and security has been proposed for only Wi-Fi network .In real-time Wi-Fi network not only high guarantee ratio or packet delivery ratio is required for packet ,but also high quality of security is need to protect data /information stored in packets transmitted through network . Our experimental results showed that the EDF packet scheduler can decrease the deadline miss rate and the traffic control mechanism can decrease network delay. Future work includes experiment the traffic control mechanism in complex network topologies and performing fine-grained network resource control, for example, adopting software-defined network techniques to prioritize messages on intermediate network devices according to message deadlines. In doing so, we wish to study the impact of our hybrid EDF and partial- EDF scheduler in a large-scale environment, where more nodes could process real-time distributed tasks simultaneously. In addition, we wish to find a better way to evaluate security on the packets.

REFERENCES

[1] Lucia Seno, Adriano, and Claudio Zunino, "A Dynamic bandwidth reassignment technique for improving QoS in the EdF-based industrial wireless network," in proc.978-1-4799-6649-3/15, IEEE 2015.

[2] W.-K. Chen, *Linear Networks, and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[3] Maen Saleh and Liang Dong, "Comparing FCFS & EDF Scheduling algorithms for real-time packet switching network," In proc.978-1-4244-6452-4/10, IEEE 2010.

[4] Xiao Qin, Mohamed Alghamdi, "Improving security of real-time wireless networks through packet scheduling," IEEE Transaction on wireless communication. Vol.7, no.9, September 2008.

[5] M. Saleh and L. Dong, “Real-Time Scheduling with Security Enhancement for Packet Switched Networks”, IEEE Transactions on Network and Service Management, 2013.

[6] Girish Tiwari and Dheeresh Mishra, “Dynamic Secure-Aware Real-Time Scheduling Algorithm for Packet Switched Network," In Proc. International Journal on recent and Innovation trends in computing and communication vol.5 issue: 2, February 2017.

[7] Xiaomin Zhu ∗, Hao Guo, Shaoshuai Liang, Xiaoling Yang, "An improved security-aware packet scheduling algorithm in real-time wireless networks," In Proc. Information Processing Letters 112, Elsevier 2012.

[8] S. Lu, V. Bharghavan, and R. Srikant, ”Fair scheduling in wireless packet networks,”IEEE Trans. Networking, Aug. 1999.

[9] M. Saleh and L. Dong, “Adaptive security-aware scheduling using Mult-Agent system”, IEEE ICC 2012-Communication QoS, Reliability and Modeling Symposium.

[10] M. Saleh and L. Dong, “Real-Time Scheduling with security Awareness for Packet Switched Network”, In proc, 978-1-4577-1155-8/12, IEEE 2012.